الگوریتم‌های رمزنگاری

و

نفوذ در شبکه

دکتر سید نورالله رواله

استاد دانشگاه آزاد اسلامی

واحد تهران شرق

۱۳۹۴

بسم الله الرحمن الرحیم

سرشناسه	: واله، سید نواله، ۱۳۲۹ -
عنوان و نام پدید آور	: الگوریتم های رمز نگاری و نفوذ در شبکه / تالیف سید نوراله واله /
مشخصات نشر	: تهران: سید نوراله واله، ۱۳۹٤.
مشخصات ظاهری	:۱۵۰ص.: مصور ، جدول ، نمودار.
شابک	:978-600-04-4285-9
وضعیت فهرست نویسی	: فیپا
عنوان اصلی	: Coding Algorithms and Penetration in Network
موضوع	: شبکه های کامپیوتری- - تدابیر ایمنی
موضوع	: آزمایش نفوذ- -(ایمن سازی کامپیوتر)
موضوع	: کامپیوترها- -ایمنی اطلاعات
موضوع	: الگوریتم های کامپیوتری
موضوع	: رمزنگاری
رده بندی کنگره	: ۱۳۹٤ ۷ الف۲و/۵۹/۵۱۰۵TK
رده بندی دیویی	۰۵/۸
شماره کتابشناسی ملی	٤
نام کتاب	: الگوریتم های رمز نگاری و نفوذ د شبکه
تالیف	: دکتر سید نوراله واله
ناشر	: ناشر مولف دکتر سید نوراله واله
نوبت چاپ	: اول
چاپ	: مهدی
تیراژ	: ۵۰۰ نسخه
قیمت	: ۱۰۰،۰۰۰ ریال
تاریخ انتشار	: ۱۳۹٤
شابک	: ۹-۴۲۸۵-۰٤-۶۰۰-۹۷۸

شابک: ۹-۴۲۸۵-۰۴-۶۰۰-۹۷۸

ISBN: 978-600-04-4285-9

تلفن: ۰۹۱۲٤٤۳۰۸٤۰ - ۸۸۲۵٤۳۰۰

مقدمه

رخنه کردن یا هک به معنی سود بردن از یک روش سریع و هوشمندانه برای حل یک مشکل در رایانه که رمزگشایی (crack) است نیز میباشد. در علوم مربوط به رایانه معنی هک گاه مساوی معنی کرک عنوان میشود. در گفتگوهای امروزی هک به معنی نفوذ به یک سیستم رایانه‌ای است و کرک نیز به معنی رمزگشایی است و کراکر به فرد گشاینده رمز میگویند.

گستردگی واژه هک منحصر به رایانه نمیباشد وتوسط افراد با تخصص‌های گوناگون در زمینه‌هایی از قبیل موسیقی، نقاشی و... نیز به کار می‌رود که به معنی دگرگونی‌های هوشمندانه و خلاقانه فرد در آن زمینه می‌باشد.

معنی اصلی آن سود بردن از یک روش سریع و هوشمندانه برای حل مشکلی تکنیکی بوده است. این واژه همواره با واژه مشتق شده دیگر آن هکر، به معنی کسی می‌باشد که توانایی پیاده سازی و ساخت هک‌های جدید را دارد. امنیت شبکه، به معنای حفاظت فیزیکی تنها نیست، بلکه یک مسئول امنیت شبکه باید بتواند از نظر سایبری نیز از آن دفاع کند و بابهره گیری از مسائل به روز شده ریاضیات و منطق، همچنین نرم افزارهای جاسوسی و ضدجاسوسی معتبر و به روز شده و بهره گیری از مسائل روز رمزنگاری و امضاهای دیجیتال، بتوانند از شبکه دفاع کامل کنند.

اگر به عنوان یک مشاور امنیتی، یک مسئول امنیت شبکه، یک مسئول شبکه وحتی یک کاربرخانگی پا به عرصه سایبری و دنیای پراز خطر و هیجان صفر و یک بگذارید بهتر است ابتدا با مسائل امنیتی آشنا شده، سپس علم خود را در این راستا افزایش دهید و با به روز رسانی مداوم علم خود، قدرت سایبری خود را به جهان معرفی نمایید. در مجموع شناخت الگوریتم‌های رمزنگاری به عنوان مهمترین عامل نرم در شبکه می‌باشد که در این مجموعه مورد بررسی قرار گرفته‌اند. امید است این مجموعه مؤثر و مفید واقع گردد.

دکتر سید نوراله واله

استاد دانشگاه آزاد اسلامی واحد تهران شرق

۱۳۹۴

فهرست مطالب

عنوان — صفحه

فصل اول

فصل دوم

فصل سوم

فصل چهارم